Dual Antenna Selection in Secure Cognitive Radio Networks

Gaojie Chen, Yu Gong, *Member, IEEE*, Pei Xiao, *Senior Member, IEEE*
and Jonathon Chambers, *Fellow, IEEE*

***Abstract*—This paper investigates data transmission and physical layer secrecy in cognitive radio network. We propose to apply full duplex transmission and dual antenna selection at secondary destination node. With the full duplex transmission, the secondary destination node can simultaneously apply the receiving and jamming antenna selection to improve the secondary data transmission and primary secrecy performance respectively. This describes an attractive scheme in practice: unlike that in most existing approaches, the secrecy performance improvement in the CR network is no longer at the price of the data transmission loss. The outage probabilities for both the data transmission and physical layer secrecy are analyzed. Numerical simulations are also included to verify the performance of the proposed scheme.**

***Index Terms*—Physical layer secrecy, cognitive radio network, antenna selection, full duplex**

I. Introduction

Cognitive radio (CR) improves spectrum utilization by sharing resources between primary and cognitive radio (secondary) users. Among various spectrum sharing schemes including underlay, overlay and interweave, the underlay scheme is often of interest in practical implementation [1]. In the underlay approach, the secondary user is allowed to access the spectrum of the primary user if its interference to the primary user is below a certain level. It is known that the antenna selection provides an attractive approach in the underlay CR network [2]–[4]. In the CR antenna selection schemes, the 'best' antenna with the least interference to the primary users and strongest link for the secondary data transmission is often selected among a number of available antennas equipped at the secondary users.

An important issue that has attracted much attention recently is the physical layer network security in the CR system. Unlike the traditional cryptographic security system [5], the physical network security is based on Shannon theory using channel coding to achieve secure transmission [6]–[11]. The physical layer security has been investigated in various systems including direct point-to-point transmission (e.g. [12]), distributed beamforming in cooperative networks (e.g. [13], [14]), cooperative jamming (e.g. [15]–[17]), relay and jammer selection (e.g. [18]–[20]) and buffer aided relay network [21].

The physical layer secrecy is of particularly interest in the CR network. This is because that the primary users are designed to share the spectrum with secondary users, making it also 'convenient' for eavesdroppers to intercept the informative data. In [22], the secondary source is used as a jammer to improve the secrecy performance of the primary network. This is not a typical CR network as the secondary user does not transmit its own data. In [23], a CR network with multiple secondary users is considered, where the secondary user which maximizes the secrecy performance of the secondary network is selected for data transmission. In [24], transmission powers are carefully allocated between the primary and secondary users to balance the primary and secondary secrecy rates. Similarly in [25], powers are optimally allocated to maximize the secrecy rate in a MIMO cognitive network, which is achieved with distributed beamforming at the source or the relay. All of these approaches mainly focus on the physical layer secrecy in the CR network. This motives us to investigate approaches which can improve the physical layer secrecy and data transmission at the same time.

In this paper, we propose a dual antenna selection to improve data transmission in the secondary network and secrecy performance in the primary network simultaneously. This is achieved by equipping full duplex multiple antennas at the secondary destination. Full duplex transmission, which was previously considered difficult to implement due to the associated self interference, is now an attractive alternative in many applications because of the recent advances in the fields of antenna technology and signal processing [26]–[28]. In this paper, the receiving antenna selection at the secondary destination node is used to maximize the data transmission capacity in the secondary network. On the other hand, because of the full duplex transmission, the transmission antenna selection is also used at the secondary destination to transmit jamming signals to the eavesdropper so that the secrecy capacity of the primary network is improved. With the full-duplex dual antenna selection at the secondary destination, unlike existing approaches, the secrecy and data transmission performance no longer have to compromise for each other but can be improved simultaneously. This describes a new way in applying full-duplex (beside its capability in increasing data rate), which is of particular interest in 5G applications including CR network, D2D transmission and small cell systems.

The main contributions of this paper are summarized as

G. Chen and P. Xiao are with the Institute for Communication Systems (ICS), Home of 5G Innovation Centre, University of Surrey, Guildford, Surrey, UK, Emails: {gaojie.chen, p.xiao}@surrey.ac.uk.

Y. Gong is with the Advanced Signal Processing Group, School of Electronic, Electrical and Systems Engineering, Loughborough University, Loughborough, Leicestershire, UK, Email: y.gong@lboro.ac.uk.

J. A. Chambers is with the Communications, Sensors, Signal and Information Processing Group, Newcastle University, Newcastle Upon Tyne, UK, E-mails: jonathon.chambers@ncl.ac.uk

follows:

- Proposing the full duplex dual antenna selection scheme to improve the data transmission for the secondary network and secrecy performance for the primary network simultaneously. Both cases with and without the knowledge of the jamming channel gains are considered. As far as the authors are aware, this is the first attempt to simultaneously improve the secrecy and data transmission in the CR network.
- Deriving the closed-form expressions the outage probability for the secondary data transmission. The analysis shows that the receiving antenna selection provides diversity gain in the secondary data transmission.
- Deriving the upper and lower bounds of the secrecy outage probability for the primary network. The analysis shows that, even without the knowledge of the jamming channel gains, the jamming antenna selection can still improve the secrecy performance of the primary network.
- Analyzing the secrecy diversity order and coding gain for the primary network, and concluding that the secrecy performance improvement from the jamming antenna selection comes from the coding gain rather than the diversity gain. This is very different from the traditional antenna selection schemes for data transmission, where the performance gain is mainly from the diversity gain. The results provide very useful insight in designing practical secrecy systems.

The remainder of the paper is organized as follows: Section II describes the dual antenna selection schemes; Section III analyzes the outage probability for the secondary data transmission; Section IV derives the upper and lower bounds of the secrecy outage probability for the primary network; Section V analyzes the secrecy diversity order and coding gain for the primary network; Section VI verifies the proposed antenna selection scheme with numerical simulations; finally Section VII summarizes the paper.

II. Dual antenna selection at the secondary destination

The system model of the secure cognitive network is shown in Fig. 1, which consists of the primary network (including one primary source node PS and one primary destination PD), the secondary network (including one secondary source node SS and one secondary destination node SD), and one eavesdropper E. The secondary destination SD performs in the full duplex mode, and is equipped with multiple antennas, where there are K_1 antennas for receiving data from the secondary source and K_2 antennas for transmitting jamming signals to the eavesdropper. All other nodes are equipped with a single antenna and perform in the half duplex mode.

We denote SD_i and SD_j as the ith and jth receiving and jamming antennas at node SD, where $i = 1, \cdots, K_1$ and $j = 1, \cdots, K_2$, respectively. As is illustrated in Fig. 1, the channel coefficients for $SS \to SD_i$, $SS \to E$, $SS \to PD$, $SD_j \to PD$, $SD_j \to E$, $PS \to SD_i$, $PS \to PD$, $PS \to E$ and $SD_j \to SD_i$ are denoted as h_{sd_i}, h_{se}, h_{sp}, h_{d_jp}, h_{d_je}, h_{pd_i}, h_{pp}, h_{pe} and $h_{d_jd_i}$, respectively.

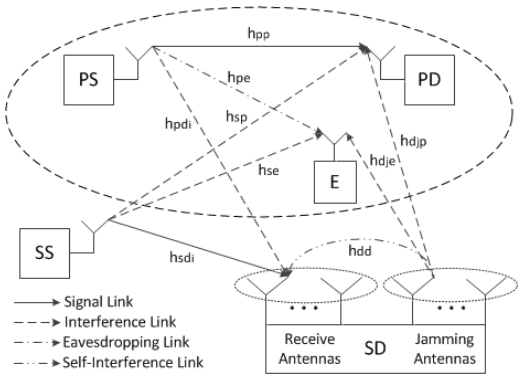


Fig. 1. Dual antenna selection in the secure CR network.

The channel gains are denoted as $\gamma_{ab} = |h_{ab}|^2$ correspondingly, which are independently exponentially distributed with mean of $\lambda_{ab} = \mathrm{E}[|h_{ab}|]^2$, where $ab \in \{sd_i, se, sp, d_jp, d_je, pd_i, pp, pe, d_jd_i\}$. We assume that $\lambda_{sd_i} = \lambda_{sd}$, $\lambda_{pd_i} = \lambda_{pd}$, $\lambda_{d_jp} = \lambda_{dp}$ and $\lambda_{d_je} = \lambda_{de}$, for all $i = 1, \cdots, K_1$ and $j = 1, \cdots, K_2$.

Without losing generality, we assume the transmission power at PS and noise variances are all normalized to unity, and the channels are quasi-static so that the channel coefficients remain unchanged during one packet duration but independently vary from one packet time to another. We also assume the secondary users have knowledge of the channel-state-information (CSI) between the secondary and primary users. This can be achieved by feeding back CSI from the primary user to the secondary transmitter directly or indirectly by, for example, a band manager between the two parties [29], or sensing pilot signals from primary users [30].

A. Receiving antenna selection

The receiving antenna is selected with the best data transmission performance in the secondary network. Because the secondary destination SD operates in full-duplex mode, it receives data from the secondary source SS and transmit jamming signals to the eavesdropper E at the same time. If the jth jamming antenna SD_j is selected, the received signal at the ith receiving antenna SD_i is given by

$$y_{sd_i} = \sqrt{P_{ss}} h_{sd_i} s_s + h_{pd_i} s_p + \sqrt{P_{sd}} h_{d_jd_i} s_t + n_{sd_i}, \quad (1)$$

where s_s, s_p and s_t are the transmission signals from nodes SS, PS and the SD_j respectively, P_{ss} and P_{sd} are the transmission powers at SS and SD respectively. It is clear that third term at the right hand side of (1) is the residual self-interference from the SD_j to SD_i.

Then the capacity for data receiving at SD_i is given by

$$C_{sd,i} = \log_2 \left(1 + \frac{P_{ss}\gamma_{sd_i}}{\gamma_{pd_i} + P_{sd}\gamma_{d_id_i} + 1} \right). \quad (2)$$

Considering that current technology can significantly suppress the self interference to the noise level (e.g [31], [32]), we assume that residual self-interference term $P_{sd}\gamma_{d_id_i}$ has little effect on $C_{sd,i}$. Further assuming the channel SNR is

high enough, we approximately have

$$C_{sd,i} \approx \log_2\left(1+\frac{P_{ss}\gamma_{sd_i}}{\gamma_{pd_i}}\right). \quad (3)$$

In the underlay CR system, the interfering power from the secondary network to the primary destination must be below a certain level. Similar to those in [23], [33], the transmission powers of SS and SD can be constrained as $P_{ss}\gamma_{sp} \le I_{th}$ and $P_{sd}\gamma_{d_jp} \le I_{th}$ respectively. Then replacing P_{ss} in (3) with I_{th}/γ_{sp} gives

$$C_{sd,i} \approx \log_2\left(1+\frac{I_{th}}{\gamma_{sp}}\cdot\frac{\gamma_{sd_i}}{\gamma_{pd_i}}\right). \quad (4)$$

Thus we propose that the receiving antenna at the secondary destination SD is selected maximizing (4) such that

$$i_r = \arg\max_{i=1,\cdots,K_1}\left\{\frac{\gamma_{sd_i}}{\gamma_{pd_i}}\right\}. \quad (5)$$

B. Jamming antenna selection

The jamming antenna is selected with the best secrecy performance in the primary network. Below we first derive the secrecy capacity for the primary network, from which the jamming selection rules are proposed.

1) Data transmission capacity at PD: Because the secondary destination SD performs in the full duplex mode, the secondary source SS transmits data and SD transmits jamming signals at the same time. Thus both SS and SD impose interference to the primary destination PD. If the jth antenna SD_j is selected, the received signal at PD is given by

$$y_{pd,j} = h_{pp}s_p + \sqrt{P_{ss}}h_{sp}s_s + \sqrt{P_{sd}}h_{d_jp}s_t + n_{pd}, \quad (6)$$

where n_{pd} is the noise at node PD. Then the capacity for data transmission at PD is obtained as

$$C_{d,j} = \log_2\left(1+\frac{\gamma_{pp}}{P_{ss}\gamma_{sp}+P_{sd}\gamma_{d_ip}+1}\right). \quad (7)$$

Using the CR power constraints in (7), we have

$$C_d = \log_2\left(1+\frac{\gamma_{pp}}{2I_{th}+1}\right) \approx \log_2\left(\frac{\gamma_{pp}}{2I_{th}+1}\right), \quad (8)$$

where the approximation holds at high SNR, and the jamming antenna index j is ignored because (8) holds for every SD_j. We note that it is common to assume high SNR in the physical layer secrecy systems to focus on the secrecy performance (e.g. [18], [21]).

2) Eavesdropping capacity at E: Due to the full-duplex transmission at SD, the eavesdropper receives signals from PS, SS and SD simultaneously. If jth jamming antenna SD_j is selected, the received signal at the eavesdropper E is given by

$$y_{e,j} = h_{pe}s_p + \sqrt{P_{ss}}h_{se}s_s + \sqrt{P_{sd}}h_{d_je}s_t + n_e, \quad (9)$$

where n_e is the noise at the eavesdropper E.

While the jamming signal s_t imposes interference on the eavesdropper E, the transmission from PS and SS forms an multiple-access channel at E. But unlike the typical multiple-access channel, for the secrecy performance of the primary network, the eavesdropper intends to 'intercept' the data from the primary source PS (and not that from the secondary source SS). Therefore, the eavesdropping capacity for the primary data s_p detection is a piece-wise function of the $SS \to E$ channel gain γ_{se} as is shown in the following. We suppose the data rate of the secondary source SS is R_{data}.

- If $\log_2(1+\frac{P_{ss}\gamma_{se}}{P_{sd}\gamma_{d_je}+1}) < R_{data}$, the $SS \to E$ channel is too weak for the eavesdropper to decode the secondary data s_s, so that s_s can only be treated as interference. Then the eavesdropping capacity for the primary network is obtained as

$$C_{e,j} = \log_2\left(1+\frac{\gamma_{pe}}{P_{ss}\gamma_{se}+P_{sd}\gamma_{d_je}+1}\right), \quad \text{if} \quad P_{ss}\gamma_{se} < (2^{R_{data}}-1)(P_{sd}\gamma_{d_je}+1). \quad (10)$$

- If $\log_2(1+\frac{P_{ss}\gamma_{se}}{\gamma_{pe}+P_{sd}\gamma_{d_je}+1}) < R_{data} < \log_2(1+\frac{P_{ss}\gamma_{se}}{P_{sd}\gamma_{d_je}+1})$, the eavesdropper can jointly decode the data from PS and SS. Considering that SS transmits at rate R_{data}, the eavesdropping capacity for the primary network is obtained as

$$C_{e,j} = \log_2\left(1+\frac{\gamma_{pe}+P_{ss}\gamma_{se}}{P_{sd}\gamma_{d_je}+1}\right) - R_{data}, \quad \text{if } (2^{R_{data}}-1)(P_{sd}\gamma_{d_je}+1) < P_{ss}\gamma_{se} < (2^{R_{data}}-1)(\gamma_{pe}+P_{sd}\gamma_{d_je}+1). \quad (11)$$

  where the first term at the right-hand-of (11) is the 'overall' capacity for the s_p and s_s detection.
- If $\log_2(1+\frac{P_{ss}\gamma_{se}}{\gamma_{pe}+P_{sd}\gamma_{d_je}+1}) > R_{data}$, the $SS \to E$ channel is strong enough for the eavesdropper to decode s_s first (by treating s_p as interference). The eavesdropper then subtracts the s_s term from its received signal (which is given by (9)), and decodes s_p. Then the eavesdropping capacity for the primary network is obtained as if there is no SS transmission as

$$C_{e,j} = \log_2\left(1+\frac{\gamma_{pe}}{P_{sd}\gamma_{d_je}+1}\right), \quad \text{if} \quad P_{ss}\gamma_{se} > (2^{R_{data}}-1)(\gamma_{pe}+P_{sd}\gamma_{d_je}+1). \quad (12)$$

3) Secrecy capacity: If the j jamming antenna SD_j is selected, the secrecy capacity ([8]) in the primary network is obtained as

$$C_{s,j} = [C_d - C_{e,j}]^+, \quad (13)$$

where $[a]^+ = \max(a, 0)$.

It is clear from (13) that, in order to have large secrecy capacity, the jamming antenna at the secondary destination need to be selected corresponding to large data transmission capacity C_d at PD and small eavesdropping capacity $C_{e,j}$ at E. Or the selected antenna has high 'jamming' to E and low 'interference' to PD. This again requires large $|h_{d_je}|^2$ and small $|h_{d_jp}|^2$, as is shown in (7) and (10-12), respectively. Thus we propose to select the jamming antenna with the largest ratio of $\gamma_{d_je}/\gamma_{d_jp}$. In fact, as will be shown later in (25) and (26), this jamming antenna selection scheme maximizes the upper and lower bounds of the secrecy capacity.

4) Jamming antenna selection rules: We assume that the secondary destination SD is aware of the $SD_j \to PD$ channel gains $\gamma_{d_j p}$. Then depending on the knowledge of the $SD_j \to E$ jamming channel gains, we propose two jamming antenna selection rules:

Case 1 - If the knowledge of the $SD_j \to E$ jamming channel gains is available, the jamming antenna is selected to satisfy

$$j_{\text{case 1}} = \arg \max_{j=1,\cdots,K_2} \left\{ \frac{\gamma_{d_j e}}{\gamma_{d_j p}} \right\}. \tag{14}$$

Case 2 - If the knowledge of the $SD_j \to E$ jamming channel gains is not available (which is often the case in practice), the jamming antenna is selected to satisfy

$$j_{\text{case 2}} = \arg \max_{j=1,\cdots,K_2} \left\{ \frac{1}{\gamma_{d_j p}} \right\}. \tag{15}$$

Below, we drive the outage probabilities for the data transmission in the secondary network and secrecy performance in the primary network.

III. Outage probability of the secondary data transmission

This section analyzes the outage probability of the data transmission in the secondary network. If the ith receiving antenna SD_i is selected at the secondary destination, the data transmission capacity in the secondary network is given by (4) when the channel SNR is high enough. Because the receiving antenna is selected from K_1 antennas, and from (5), the capacity for the data transmission is approximately given by

$$C_{sd} \approx \log_2 \left(1 + I_{th} \cdot \frac{\max\limits_{i=1,\cdots,K_1} \left(\frac{\gamma_{sd_i}}{\gamma_{pd_i}} \right)}{\gamma_{sp}} \right). \tag{16}$$

The outage probability for data transmission in the secondary network is then given by

$$P_{d,out} = P(C_{sd} < R_{data}), \tag{17}$$

where R_{data} is the data rate at the secondary source SS.

Substituting (16) into (17) and letting $X_1 = \max\limits_{i=1,\cdots,K_1} \left(\frac{\gamma_{sd_i}}{\gamma_{pd_i}} \right)$, $Y_1 = \gamma_{sp}$, $Z_1 = X_1/Y_1$ and $z_1 = \frac{2^{R_{data}}-1}{I_{th}}$, we have

$$\begin{aligned} P_{d,out} &= F_{Z_1}(z_1) = P\left(X_1/Y_1 < z_1\right) \\ &= \int_0^\infty F_{X_1}(z_1 y_1) f_{Y_1}(y_1) dy_1, \end{aligned} \tag{18}$$

where $F(.)$ is the cumulative density function (CDF).

The CDF of X_1 and probability density function (PDF) of Y_1 can be obtained as

$$F_{X_1}(x_1) = \left[\frac{x_1}{N + x_1} \right]^{K_1} \quad \text{and} \quad f_{Y_1}(y_1) = \frac{1}{\lambda_{sp}} e^{-\frac{y_1}{\lambda_{sp}}}, \tag{19}$$

respectively, where $N = \lambda_{sd}/\lambda_{pd}$.

Finally, substituting (19) into (18) gives

$$P_{d,out} = \begin{cases} 1 - \frac{N}{\lambda_{sp} z_1} e^{\frac{N}{\lambda_{sp} z_1}} \text{Ei}(1, \frac{N}{\lambda_{sp} z_1}), \\ \qquad\qquad \text{if} \quad K_1 = 1, \\ \left(\frac{\lambda_{sp} z_1}{N} \right)^{K_1 - 1} \frac{\mathcal{MG}\left([[0], [\ ]], [[K_1 - 1, K_1], [\ ]], \frac{N}{\lambda_{sp} z_1} \right)}{\Gamma(K_1)}, \\ \qquad\qquad \text{if} \quad K_1 \geq 2, \end{cases} \tag{20}$$

where $\text{Ei}(1, a) = \int_1^\infty \frac{\exp(-ta)}{a} dt, a > 0$, $\Gamma(\bullet)$ is the gamma function, and $\mathcal{MG}\left([[\ ], [\ ]], [[\bullet, \bullet], [\ ]], \bullet \right)$ is the Meijer G function [34].

It is clear from (20) that the outage probability $P_{s,out}$ well depends on N, or a larger N leads to smaller outage probability. It is thus of interest to show the diversity order for the data transmission in the secondary network which is defined as

$$d_d = -\lim_{N \to \infty} \frac{\log_{10} P_{d,out}}{\log_{10} N}. \tag{21}$$

We note that the definition in (21) is similar to that of the conventional diversity order except now the SNR is replaced with the parameter N. The diversity order defined in (21) reflects the decreasing rate of $P_{s,out}$ with respect to the receiving antenna number K_1.

Unfortunately, because (20) contains the Meijer G function $\mathcal{MG}(.)$, it is very hard to derive the diversity order. On the other hand, numerical results show that $\mathcal{MG}(.)$ has little effect on the diversity order. Then ignoring the $\mathcal{MG}(.)$ term in (20), we approximately have

$$d_d \approx -\lim_{N \to \infty} \frac{\log_{10} (\lambda_{sp} z_1 / N)^{K_1 - 1}}{\log_{10} N} = K_1 - 1, \qquad K_1 \geq 2. \tag{22}$$

This shows that the receiving antenna selection introduces diversity gain in the data transmission, which is similar to that in the traditional antenna selection schemes [4]. This result will be verified in the simulation later.

IV. Secrecy outage probability of the primary network

This section analyzes the secrecy outage probability of the primary networks. Both Case 1 and 2, with and without the knowledge of the jamming channel gains respectively, are considered. Because the eavesdropping capacity is a complicated piece-wise function as is shown in (10-12), it is hard (if not impossible) to obtain the closed form expression of secrecy outage probability for the primary network. Instead, the upper and lower bounds of the secrecy outage probability are derived.

First, the maximum eavesdropping capacity for the primary source $C_{e,j}$ is obtained when the signals from SS has no effect on the eavesdropper to detect the data from PS. This happens when $\gamma_{se} = 0$, or $P_{ss}\gamma_{se} > (2^{R_{data}} - 1)(\gamma_{pe} + P_{sd}\gamma_{d_j e} + 1)$ so that the $SS \to E$ link is strong enough for the eavesdropper to successfully decode ss and subtract it from the received signal. Thus when jth jamming antenna is selected, the upper bound of the eavesdropping capacity is given by

$$C_{e,j}^{(up)} = \log_2 \left(1 + \frac{\gamma_{pe}}{P_{sd}\gamma_{d_j e} + 1} \right). \tag{23}$$

On the other hand, we notice that when $\log(1+\frac{P_{ss}\gamma_{se}}{P_{sd}\gamma_{d_je}+1}) < R_{data}$, or $P_{ss}\gamma_{se} < (2^{R_{data}}-1)(P_{sd}\gamma_{d_je}+1)$, the eavesdropper cannot decode s_s so that the signals from SS is treated as interference. When $P_{ss}\gamma_{se} > (2^{R_{data}}-1)(P_{sd}\gamma_{d_je}+1)$, s_s and s_p (from SS and PS respectively) can be jointly decoded. Therefore, the minimum eavesdropping capacity $C_{e,j}$ is reached when $P_{ss}\gamma_{se} = (2^{R_{data}}-1)(P_{sd}\gamma_{d_je}+1)$. Substituting $P_{ss}\gamma_{se} = (2^{R_{data}}-1)(P_{sd}\gamma_{d_je}+1)$ into (10) then gives the lower bound of $C_{e,j}$ as

$$C_{e,j}^{(low)} = \log_2\left(1+\frac{\gamma_{pe}}{\Delta\cdot(P_{sd}\gamma_{d_je}+1)}\right), \tag{24}$$

where $\Delta = 2^{R_{data}}-1$.

Recall that the capacity for data transmission at the primary destination PD is given by (8). Then substituting (8), (23) and (24) into (13), and with the CR power constraints, we obtain the lower and upper bounds of the secrecy capacity for the primary network (corresponding to the jth jamming antenna) as

$$C_{s,j}^{(low)} = \left[C_d - C_{e,j}^{(up)}\right]^+ \approx \left[\log_2\left(\frac{I_{th}\gamma_{pp}\gamma_{d_je}}{(2I_{th}+1)\gamma_{pe}\gamma_{d_jp}}\right)\right]^+, \tag{25}$$

$$C_{s,j}^{(up)} = \left[C_d - C_{e,j}^{(low)}\right]^+ \approx \left[\log_2\left(\frac{\Delta\cdot I_{th}\gamma_{pp}\gamma_{d_je}}{(2I_{th}+1)\gamma_{pe}\gamma_{d_jp}}\right)\right]^+, \tag{26}$$

respectively, where the approximation holds at the high SNR which is often of interests in secrecy performance [18]. In the following two subsections, we drive the upper and lower bounds of the secrecy outage probability for Case 1 and 2 respectively.

A. Case 1 - with the knowledge of the $SD_j \to E$ jamming channel

The jamming antenna selection rule in Case 1 is shown in (14).

1) Upper bound - Case 1: Noting that the jamming antenna is selected among K_2 antennas, and from (25), the lower bound of the secrecy capacity in Case 1 is obtained as

$$C_s^{(low,\ case\ 1)} = \left[\log_2\left(\frac{I_{th}\gamma_{pp}}{(2I_{th}+1)\gamma_{pe}}\cdot\max_{j=1\cdots,K_2}\left(\frac{\gamma_{d_je}}{\gamma_{d_jp}}\right)\right)\right]^+. \tag{27}$$

Then the upper bound of the secrecy outage probability in Case 1 is given by

$$P_{s,\ out}^{(up,\ case\ 1)} = P(C_s^{(low,\ case\ 1)} < R_{secrecy}), \tag{28}$$

where $R_{secrecy}$ is the target secrecy rate.

We let $X = \max_{j=1\cdots,K_2}\left(\frac{\gamma_{d_je}}{\gamma_{d_jp}}\right)$, $Y = \frac{\gamma_{pe}}{\gamma_{pp}}$ and $Z = X/Y$. Further noting that the CDF of the division of two random variables is given by (18), the CDF of X and PDF of Y can be obtained as

$$F_X(x) = \left[\frac{x}{M+x}\right]^{K_2} \quad \text{and} \quad f_Y(y) = \frac{L}{(L+y)^2}, \tag{29}$$

respectively, where $M = \lambda_{de}/\lambda_{dp}$ and $L = \lambda_{pe}/\lambda_{pp}$.

The CDF of Z is then given by

$$F_Z(z) = \int_0^\infty F_X(zy)f_Y(y)dy. \tag{30}$$

Substituting (29) into (30) gives (31) in the top of the next page. We note that there is no uniform format of $F_Z(z)$ with respect to the number of jamming antennas K_2. But the closed form expression can be obtained for any given K_2, some of which are shown in (31).

Finally from (28), the upper bound of the secrecy outage probability of primary network is given by

$$P_{s,\ out}^{(up,\ case\ 1)} = F_Z(u), \tag{32}$$

where $u = \frac{2^{R_{secrecy}}(2I_{th}+1)}{I_{th}}$.

2) Lower bound - Case 1: On the other hand, from (14) and (26), the upper bound of the secrecy capacity in Case 1 is obtained as

$$C_s^{(up,\ case\ 1)} = \left[\log_2\left(\frac{\Delta\cdot I_{th}\gamma_{pp}}{(2I_{th}+1)\gamma_{pe}}\cdot\max_{j=1\cdots,K_2}\left(\frac{\gamma_{d_je}}{\gamma_{d_jp}}\right)\right)\right]^+. \tag{33}$$

Then the lower bound of the secrecy outage probability in Case 1 is given by

$$P_{s,\ out}^{(low,\ case\ 1)} = P(C_s^{(up,\ case\ 1)} < R_{secrecy}). \tag{34}$$

Following the same procedures as those in obtaining (32), we have

$$P_{s,\ out}^{(low,\ case\ 1)} = F_Z(v), \tag{35}$$

where $v = \frac{2^{R_{secrecy}}(2I_{th}+1)}{\Delta\cdot I_{th}}$, and $F_Z(.)$ is given by (32).

B. Case 2 - without the knowledge of the $SD_j \to E$ jamming channel

The jamming antenna selection rule in Case 2 is given by (15).

1) Upper bound - Case 2: From (15) and (25), the lower bound of the secrecy capacity is obtained as

$$C_s^{(low,\ case\ 2)} = \left[\log_2\left(\frac{I_{th}\gamma_{pp}\gamma_{d_je}}{(2I_{th}+1)\gamma_{pe}}\cdot\max_{j=1,\cdots,K_2}\left(\frac{1}{\gamma_{d_jp}}\right)\right)\right]^+. \tag{36}$$

The upper bound of the secrecy outage probability in Case 2 is then given by

$$P_{s,\ out}^{(up,\ case\ 2)} = P(C_s^{(low,\ case\ 2)} < R_{secrecy}). \tag{37}$$

We let $X_2 = \max_{j=1,\cdots,K_2}\left(\frac{1}{\gamma_{d_jp}}\right)$, $Y_2 = \frac{\gamma_{pp}}{\gamma_{pe}}$ and $W_1 = \gamma_{d_je}$. Using the order statistics, the CDF of X_2 is obtained as

$$F_{X_2}(x_2) = e^{-\frac{K_2}{\lambda_{dp}x_2}}. \tag{38}$$

The PDF-s of W_1 and Y_2 are given by

$$f_{Y_2}(y_2) = \frac{1/L}{(1/L+y_2)^2} \quad \text{and} \quad f_{W_1}(w_1) = \frac{1}{\lambda_{de}}e^{-\frac{w_1}{\lambda_{de}}}. \tag{39}$$

respectively.

Further letting $T_1 = X_2W_1$, the CDF of T_1 is given by

$$F_{T_1}(t_1) = \int_0^\infty F_{X_2}(t_1/w_1)f_{W_1}(w_1)dw_1 = \frac{\lambda_{dp}t_1}{\lambda_{de}K_2+\lambda_{dp}t_1}. \tag{40}$$

$$F_Z(z)=\begin{cases}\frac{Lz\left[Lz-M-M\ln\left(\frac{zL}{M}\right)\right]}{(Lz-M)^2}, & \text{if} \quad K_2=1,\\ \frac{Lz\left[-L^2z^2+M^2-2LMz\ln\left(\frac{zL}{M}\right)\right]}{(Lz-M)^3}, & \text{if} \quad K_2=2,\\ \frac{Lz\left[2L^3z^3+3L^2Mz^2-6LM^2z+M^3-2L^2Mz^2\ln\left(\frac{zL}{M}\right)\right]}{2(Lz-M)^4}, & \text{if} \quad K_2=3,\\ \frac{Lz\left[12L^5z^5+65Mz^4L^4-120z^3L^3M^2+60z^2L^2M^3-20zLM^4+3M^5-60L^4Mz^4\ln\left(\frac{zL}{M}\right)\right]}{12(Lz-M)^6}, & \text{if} \quad K_2=5,\\ \cdots, \end{cases} \tag{31}$$

Finally we let $Q=T_1Y_2$, and obtain the CDF of Q as

$$\begin{aligned}F_Q(q)&=\int_0^\infty F_{T_1}(q/y_2)f_{Y_2}(y_2)dy_2\\&=\frac{L\lambda_{dp}q\left[\lambda_{dp}qL-K_2\lambda_{de}-K_2\lambda_{de}\ln\left(\frac{\lambda_{dp}qL}{K_2\lambda_{de}}\right)\right]}{(K_2\lambda_{de}-\lambda_{dp}qL)^2}.\end{aligned} \tag{41}$$

Comparing (37) and (41), we then have

$$\begin{aligned}P_{s,\ out}^{(up,\ case\ 2)}&=F_Q(u)\\&=\frac{Lu\left[-MK_2+uL-MK_2\ln\left(\frac{uL}{MK_2}\right)\right]}{(MK_2-uL)^2},\end{aligned} \tag{42}$$

where $u=\frac{2^{R_{secrecy}}(2I_{th}+1)}{I_{th}}$, M and L are defined in (29).

2) Lower bound - Case 2: From (26) and (15), the upper bound of the secrecy capacity in Case 2 is obtained as

$$C_s^{(up,\ case\ 2)}=\left[\log_2\left(\frac{\Delta\cdot I_{th}\gamma_{pp}\gamma_{d_je}}{(2I_{th}+1)\gamma_{pe}}\cdot\max_{j=1,\cdots,K_2}\left(\frac{1}{\gamma_{d_jp}}\right)\right)\right]^+. \tag{43}$$

Then following the similar procedures as those in obtaining (42), we obtain the lower bound of the secrecy outage probability in Case 2 as

$$P_{s,\ out}^{(low,\ case\ 2)}=P(C_s^{(up,\ case\ 2)}<R_{secrecy})=F_Q(v), \tag{44}$$

where $v=\frac{2^{R_{secrecy}}(2I_{th}+1)}{\Delta\cdot I_{th}}$.

V. Asymptotical secrecy performance

It is shown above that, in both Case 1 and 2, the secrecy performance of the primary network depends on the ratio of $M=\frac{\lambda_{de}}{\lambda_{dp}}$, or a larger M results in better secrecy performance. In fact, M to the secrecy outage probability is similar as the SNR to the data transmission outage probability. Thus it is of great interest to analyze the asymptotical secrecy performance that is, when $M\to\infty$, how the secrecy performance varies with the number of jamming antenna K_2. Similar to the conventional data transmission, the asymptotical secrecy performance includes the secrecy diversity order and coding gain.

When $M\to\infty$, the secondary source SS transmission has little effect on the eavesdropping capacity so that the secrecy outage probability is close to the upper bound. Thus the secrecy diversity order and coding gain can be defined based on the upper bound of the secrecy outage probability. To be specific, the secrecy diversity order is defined as

$$d_s=-\lim_{M\to\infty}\frac{\log_{10}P_{s,out}^{(up)}}{\log_{10}M}. \tag{45}$$

Similar to the classic diversity order, the secrecy diversity order reflects the decreasing rate of the secrecy outage probability with respect to the antenna number K_2.

On the other hand, the secrecy coding gain can be defined as

$$\begin{aligned}c_s=&\lim_{M\to\infty}10\log_{10}P_{s,out}^{(up)}(K=K_b)\\&-\lim_{M\to\infty}10\log_{10}P_{s,out}^{(up)}(K=K_2),\end{aligned} \tag{46}$$

where $P_{s,out}^{(up)}(K)$ is the secrecy outage probability if there are K antenna available for jamming antennas selection, K_2 is the number of available jamming antennas, K_b is the number of jamming antennas in the baseline system for comparison. As will be shown below, we let $K_b=2$ and $K_b=1$ in Case 1 and Case 2 respectively. It is clear from (46) that the secrecy coding gain reflects the 'shift' of the secrecy outage probability with respect to the antenna number K_2.

A. Case 1 - with the knowledge of the $SD_j\to E$ jamming channel

From (31), and ignoring lower orders of M terms, we have

$$\lim_{M\to\infty}P_{s,\ out}^{(up,\ case\ 1)}=\begin{cases}Lz\cdot\ln(M)M^{-1}, & \text{if} \quad K_2=1,\\ \frac{Lz}{K_2-1}\cdot M^{-1}, & \text{if} \quad K_2\geq 2.\end{cases} \tag{47}$$

Substituting (47) into (45) gives the secrecy diversity order in Case 1. To be specific, if $K_2=1$, the secrecy diversity order is obtained as

$$\begin{aligned}d_s^{(case\ 1)}(K_2=1)&=-\lim_{M\to\infty}\frac{\log_{10}(Lz\cdot\ln(M)M^{-1})}{\log_{10}M}\\&=-\lim_{M\to\infty}\frac{\log_{10}(Lz)}{\log_{10}M}-\lim_{M\to\infty}\frac{\log_{10}(\ln(M))}{\log_{10}M}\\&\quad-\lim_{M\to\infty}\frac{\log_{10}(M^{-1})}{\log_{10}M}\\&=1.\end{aligned} \tag{48}$$

And if $K_2\geq 2$, the secrecy diversity order is given by

$$d_s^{(case\ 1)}(K_2\geq 2)=-\lim_{M\to\infty}\frac{\log_{10}(\frac{Lz}{K_2-1}\cdot M^{-1})}{\log_{10}M}=1 \tag{49}$$

Combining (48) and (49), we obtain the secrecy diversity order in Case 1 as

$$d_s^{(case\ 1)}=1. \tag{50}$$

On the other hand, as is shown in (47), $\lim_{M\to\infty} P_{s,\ out}^{(up,\ case\ 1)}$ has a uniform expression for $K_2 \geq 2$. Thus we let $K_b = 2$ in (46) as a baseline to define the secrecy coding gain in Case 1 as

$$\begin{aligned} c_s^{(case\ 1)} = &\lim_{M\to\infty} 10\log_{10} P_{s,\ out}^{(up,\ case\ 1)}(K=2) \\ &- \lim_{M\to\infty} 10\log_{10} P_{s,\ out}^{(up,\ case\ 1)}(K=K_2). \end{aligned} \tag{51}$$

Substituting (47) into (51) gives the secrecy coding gain in Case 1 as

$$c_s^{(case\ 1)} = 10\log_{10}(K_2 - 1), \qquad \text{for } K_2 \geq 2. \tag{52}$$

B. Case 2 - without the knowledge of the $SD_j \to E$ jamming channel

From (42), and ignoring lower orders of M terms, the asymptotic secrecy outage probability for Case 2 is given by

$$\lim_{M\to\infty} P_{s,\ out}^{(up,\ case\ 2)} = \frac{Lz}{K_2} \cdot \ln(M) M^{-1}. \tag{53}$$

Substituting (53) into (45) gives the secrecy diversity order in Case 2 as

$$d_s^{(case\ 2)} = -\lim_{M\to\infty} \frac{\log_{10}(Lz/K_2 \cdot \ln(M)M^{-1})}{\log_{10} M} = 1. \tag{54}$$

On the other hand, because (53) holds for any K_2, we let $K_b = 1$ in (46) as a baseline to define the secrecy coding gain in Case 2 as

$$\begin{aligned} c_s^{(case\ 2)} = &\lim_{M\to\infty} 10\log P_{s,\ out}^{(up,\ case\ 2)}(K=1) \\ &- \lim_{M\to\infty} 10\log P_{s,\ out}^{(up,\ case\ 2)}(K=K_2). \end{aligned} \tag{55}$$

Substituting (53) into (55) gives secrecy coding gain in Case 2 as

$$c_s^{(case\ 2)} = 10\log_{10}(K_2). \tag{56}$$

C. Discussion

It is clear from (50) and (54) that, in both Case 1 and 2, the secrecy diversity order is 1. Or the decreasing rate of the secrecy outage probability with respect to M is always 1, no matter how many transmission jamming antennas are used at the secondary destination.

On the other hand, it is shown in (52) and (56) that, with more transmission jamming antenna for selection at the secondary destination, the secrecy outage performance still improves due to the coding gain. It is interesting to note that (52) and (56) are consistent, because they are defined based on $K_b = 2$ and $K_b = 1$ as the baselines respectively.

Therefore, in both Case 1 and 2, the jamming antenna selection at the secondary destination leads to the secrecy coding gain, but not the diversity gain. This contrasts sharply with the traditional antenna selection approaches for data transmission, where the diversity order usually goes up with the antenna number. The analysis also shows that, even without the knowledge of the $SD \to E$ jamming channel gains, the secrecy performance still improves with the jamming antenna selection.

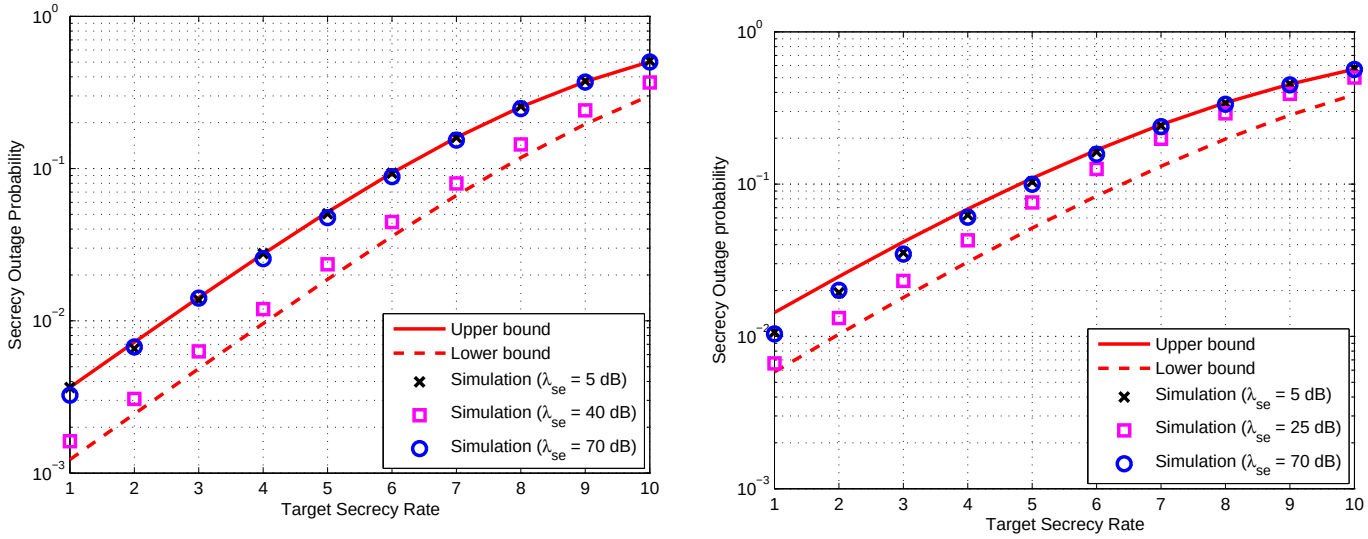
VI. Numerical simulations

In this section, we provide theoretical and simulation results to verify the proposed dual antenna selection scheme in the CR network. In the simulation, the CR network consists of one pair of primary source PS and destination PD, and one pair of secondary source SS and destination SD. Except for SD, all nodes are equipped with a single antenna. While there are multiple antennas at SD, the antenna numbers are respectively set for different simulations. All channels are Rayleigh flat fading and channel coefficients remains unchanged during one time slot but vary independently from one time slot to another. The average channel gains for different channel groups, $PS \to SD_i$, $SS \to SD_i$, $SD_i \to E$ and $SD_j \to PD$ respectively, can be different but the channels within each of the above groups are i.i.d. For example, the average channel gains for $PS \to SD_1, \cdots, PS \to SD_M$ are the same, but the average channel gains for $PS \to SD_1$ and $SS \to SD_1$ may be different. This describes a typical CR network, and the different average channel gains for each group represent different path-loss for every node at various locations within the network. All simulation results are obtained by averaging over 1,000,000 independent runs. Other parameters including the data transmission rate and target secrecy rate are set individually for every simulation.

Fig. 2 (a) and (b) show the secrecy outage probability of the primary network *vs* target secrecy rate in Case 1 and 2 respectively, where we set the number of jamming antenna as $K_2 = 5$, the average channel gains as $\lambda_{pp} = 55$ dB, $\lambda_{sp} = \lambda_{pd} = 20$ dB, $\lambda_{se} = 10$ dB, $\lambda_{pe} = 40$ dB, $\lambda_{de} = 30$ dB, $\lambda_{dp} = 20$ dB and $\lambda_{dd} = 1$ dB, the interference constraint level at the primary destination as $I_{th} = 3$ and the data transmission rate at the secondary source SS as $R_{data} = 2$ bps/Hz. Both the simulation results and theoretical upper and lower bounds are shown. It is clear that, in both cases, the simulation results lie between the lower and upper bounds, which well verifies the secrecy outage analysis for the primary network in Section IV. Specifically, when the average $SS \to E$ channel is small ($\lambda_{se} = 5$ dB) or large ($\lambda_{se} = 70$ dB), the simulation results are close to the upper bounds. This is because that, at the eavesdropper, the signals from SS can be ignored when λ_{se} is small, or successfully decoded and subtracted from the received signal when λ_{se} is large. For other $SS \to E$ channel gains, the simulation results lie between the upper and lower bounds. Comparing Fig. 2 (a) and (b) also reveals that Case 1 has better secrecy performance than Case 2. This is as expected because Case 1 has the knowledge of the $SD \to E$ jamming channel and Case 2 does not.

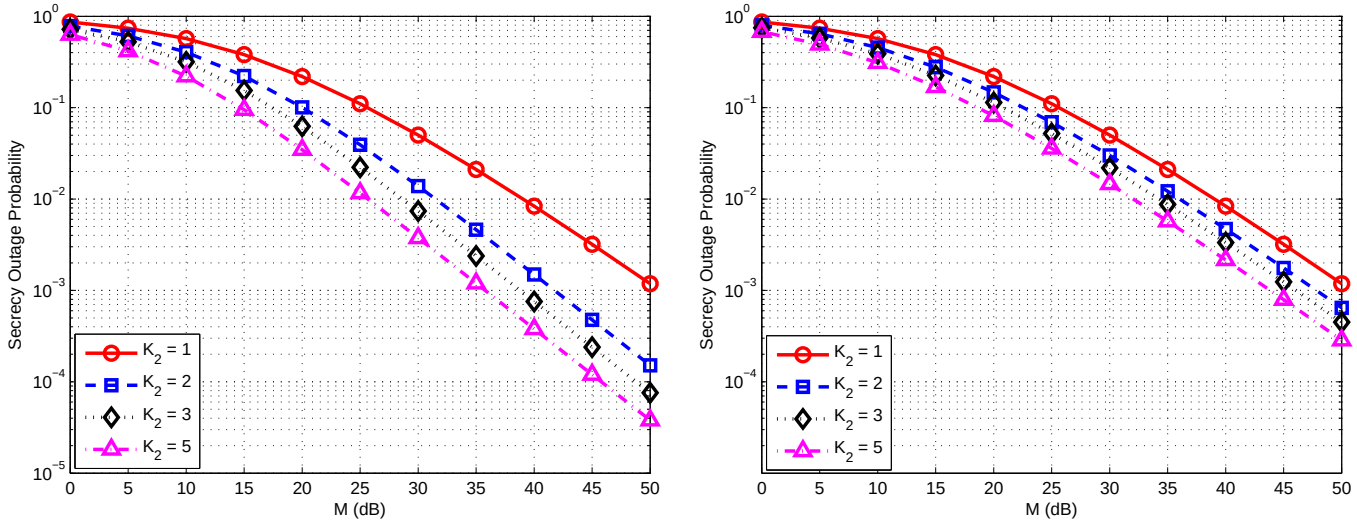
Fig. 3 shows the secrecy outage probabilities *vs* $M = \lambda_{de}/\lambda_{dp}$, where we set $I_{th} = 1$, the secrecy target rate as $R_{st} = 4$ bps/Hz and the average gain ratio $L = \lambda_{pe}/\lambda_{pp} = -5$ dB. Fig. 3 verifies the following analsyis.

- In both Case 1 and 2, the secrecy performance of the primary network improves with more jamming antennas.
- In both Case 1 and 2, the secrecy diversity orders for all jamming antenna numbers K_2 are always 1, as are given by (50) and (54) respectively. For example, for $K_2 = 5$ in Case 1, when M increases from 40 to 50 dB, the



(a) Case 1 (b) Case 2

Fig. 2. The secrecy outage probabilities *vs* target secrecy rate with $K_2 = 5$.



(a) Case 1 (b) Case 2

Fig. 3. The secrecy outage probabilities for two cases *vs* $M = \lambda_{de}/\lambda_{dp}$ (dB).

secrecy outage probability approximately drops from -37 to -47dB.

- In Case 1, the secrecy coding gain is $10\log_{10}(K_2 - 1)$, as is given by (52). For example, for $M = 50$ dB, the secrecy outage difference between $K_2 = 2$ and $K_2 = 5$ is about 6 dB, which well matches the theoretical coding gain for $K_2 = 5$ as $10\log_2(5-1) \approx 6$ dB. Note that in Case 1, the baseline system for coding gain definition is based on $K_2 = 2$.
- In Case 2, the secrecy coding gain is $10\log_{10}(K_2)$, as is given by (56). For example, for $M = 50$ dB, the secrecy outage difference between $K_2 = 5$ and $K_2 = 1$ is about 7 dB, which well matches the theoretical coding gain for $K_2 = 5$ as $10\log_{10}(5) \approx 7$ dB. Note that in Case 1, the baseline system for coding gain definition is based on $K_2 = 1$.

Thus Fig. 3 clearly shows that, in both Case 1 and 2, the jamming antenna selection at the secondary destination leads to coding gain rather than the diversity gain in the secrecy outage probability.

Fig. 4 shows the outage probability for data transmission in the secondary network *vs* $N = \lambda_{sd}/\lambda_{pd}$, where we set the target data rate in the secondary network as $R_t = 4$ bps/Hz, $\lambda_{sp} = \lambda_{pd} = 20$ dB, the power constraint level as $I_{th} = 1$ or 3. Both the simulation and theoretical results are presented, which are shown perfectly match. It is clearly shown in Fig. 4 that, for both $I_{th} = 1$ and 3, the outage probability decreases with more receiving antennas and the improvement is clearly

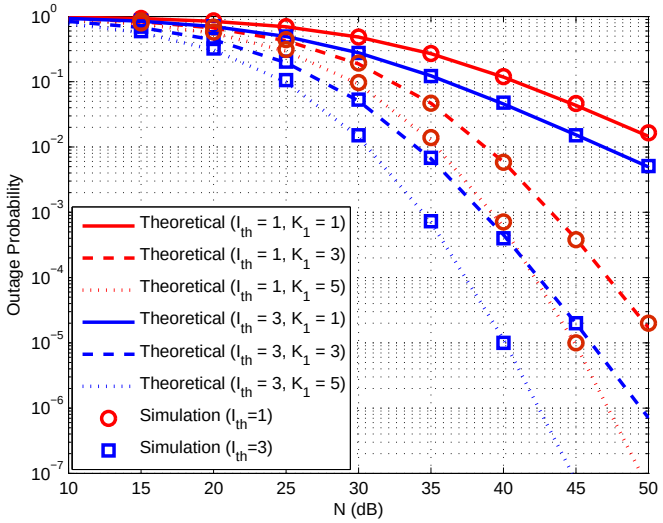


Fig. 4. The outage probability *vs* $N = \lambda_{sd}/\lambda_{pd}$ of the data transmission in the secondary network.

from the diversity gain. This well verifies the analysis in Section III that the antenna selection leads to the diversity gain for the data transmission in the secondary network.

VII. Conclusions

This paper proposed the dual antenna selection scheme in the secure CR network. This was achieved by applying full duplex transmission at the secondary user. The outage probability for both the data transmission in the secondary network and secrecy performance in the primary network were analyzed, where the analysis showed that the antenna selection leads to diversity gain for the secondary data transmission and coding gain for the primary secrecy performance respectively. Numerical simulation results were also shown to well verify the analysis in this paper. Both the analysis and simulations showed that the proposed scheme describes an attractive scheme in the secure CR network.

Acknowledgements

We would like to thank the anonymous reviewers and the editor for their constructive comments. We also would like to acknowledge the support of the University of Surrey 5GIC (http://www.surrey.ac.uk/5gic) members for this work.

References

[1] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognative radios: an information theoretic perspective," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894–914, May. 2009.

[2] R. Sarvendranath and N. B. Mehta, "Antenna selection with power adaptation in interference-constrained cognitive radios," *IEEE Trans. Commun.*, vol. 62, no. 3, pp. 786–796, Feb. 2014.

[3] M. F. Hanif, P. J. Smith, D. P. Taylor, and P. A. Martin, "MIMO cognitive radios with antenna selection," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3688–3699, Sep. 2011.

[4] R. Sarvendranath and N. B. Mehta, "Antenna selection in interference constrained underlay cognitive radios: Sep-optimal rule and performance benchmarking," *IEEE Trans. Commun.*, vol. 61, no. 2, pp. 496–506, Feb. 2013.

[5] E. D. Silva, A. L. D. Santos, L. C. P. Albini, and M. Lima, "Identity-based key management in mobile ad hoc networks: Techniques and applications," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 46–52, Oct. 2008.

[6] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[7] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[8] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[9] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[10] I. Csiszr and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2437–2452, June 2008.

[11] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.

[12] F. Renna, N. Laurenti, and H. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 4, pp. 1354–1367, Aug. 2012.

[13] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," *in Proc. 46th Ann. Allerton Conf. Communication, Control, and Computing, UIUC, Illinois*, Sep. 2008.

[14] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Amplify-and-forward based cooperation for secure wireless communications," *in Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Taipei, Taiwan*, Apr. 2009.

[15] E. Tekin, "The Gaussian multiple access wire-tap channel:wireless secrecy and cooperative jamming," *in Proc. Information Theory and Applications Workshop, La Jolla, CA*, pp. 404–413, Feb. 2007.

[16] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[17] Z. Ding, M. Peng, and H. H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461–3471, Nov. 2012.

[18] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[19] G. Chen, V. Dwyer, I. Krikidis, J. S. Thompson, S. McLaughlin, and J. A. Chambers, "Comment on 'Relay selection for secure cooperative networks with jamming'," *IEEE Trans. Wireless Commun.*, vol. 11, no. 6, pp. 2351–2351, June 2012.

[20] J. C. Chen, R. Q. Zhang, L. Y. Song, Z. Han, and B. L. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[21] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inform. Forensics and Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.

[22] Z. Shu, Y. Yang, Y. Qian, and R. Hu, "Impact of interference on secrecy capacity in a cognitive radio network," *in Proc. IEEE Globecom, Houston, USA*, Apr. 2011.

[23] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

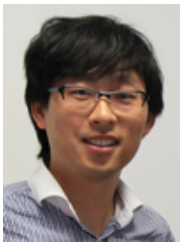
[24] Y. Wu and K. Liu, "An information secrecy game in cognitive ratio networks," *IEEE Trans. Inform. Forensics and Security*, vol. 6, no. 3, pp. 831–842, Sep. 2011.

[25] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, "Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for peimary users," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1058–1073, Feb. 2014.

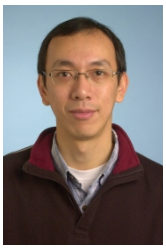
[26] B. Debaillie, D. J. Broek, C. Lavin, B. Liempd, E. A. M. Klumperink, C. Palacios, J. Craninckx, B. Nauta, and A. Parssinen, "Analog/RF solutions enabling compact full-duplex radios," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1622–1673, June 2014.

[27] S. Hong, J. Brand, J. Choi, M. Jain, J. Mehlman, S. Katti, and P. Levis, "Aplications of self-interference cancellation in 5G and beyond," *IEEE Commun. Magazine*, vol. 52, no. 2, pp. 114–121, Feb. 2014.

[28] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," *ACM SIGCOMM, Hong Kong, China*, Aug. 2013.
[29] A. Ghasemi and E. S. Sousa, "Fundamental limits of spectrum-sharing in fading environments," *IEEE Trans. Commun.*, vol. 6, no. 2, pp. 649–658, Feb. 2007.
[30] J. M. Peha, "Approaches to spectrum sharing," *IEEE Commun. Mag.*, vol. 43, no. 2, pp. 10–12, Feb. 2005.
[31] C. R. Anderson, S. Krishnamoorthy, C. G. Ranson, T. J. Lemon, W. G. Newhall, T. Kummetz, and J. H. Reed, "Antenna isolation, wideband multipath propagation measurements and interference mitigation for on-frequency repeaters," *in Proc. IEEE SoutheastCon*, Mar. 2004.
[32] H. Ju, E. Oh, and D. Hong, "Improving efficiency of resource usage in two-hop full duplex relay systems based on resource sharing and interference cancellation," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 3933–3938, Aug. 2009.
[33] G. Chen, Y. Gong, and J. A. Chambers, "Study of relay selection in a multi-cell cognitive network," *IEEE Wireless Commun. Lett.*, vol. 11, no. 6, pp. 2351–2354, June 2012.
[34] A. Gilat and V. Subramaniam, "Numerical methods for engineers and scientists: An introduction with applications using Matlab," *John Wiley Sons Ltd*, 2011.



Gaojie Chen (S'09-M'12) received the B. Eng. and B. Ec. in Electrical Information Engineering and International Economics and Trade from the Northwest University, Shaanxi, China, in 2006, and the M.Sc (Distinction) and Ph.D degrees from Loughborough University, Loughborough, UK, in 2008 and 2012, respectively, all in Electrical and Electronic Engineering. From 2008 to 2009 he worked, as a software engineering in DTmobile, Beijing, China, and from 2012 to 2013 as a Research Associate in the School of Electronic, Electrical and Systems Engineering at the Loughborough University, Loughborough, UK. Then he was a Research Fellow with the 5GIC, the Faculty of Engineering and Physical Sciences, University of Surrey, U.K., from 2014 to 2015. He is currently a Research Associate with the Department of Engineering Science, University of Oxford, U.K. His current research interests include information theory, wireless communications, cooperative communications, cognitive radio, secrecy communication and random geometric networks.



Yu Gong is with School of Electronic, Electrical and Systems Engineering, Loughborough University, UK, in July 2012. Dr Gong obtained his BEng and MEng in electronic engineering in 1992 and 1995 respectively, both at the University of Electronics and Science Technology of China. In 2002, he received his PhD in communications from the National University of Singapore. After PhD graduation, he took several research positions in Institute of Infocomm Research in Singapore and Queens University of Belfast in the UK respectively. From 2006 and 2012, Dr Gong had been an academic member in the School of Systems Engineering, University of Reading, UK. His research interests are in the area of signal processing and communications including wireless communications, cooperative networks, non-linear and non-stationary system identification and adaptive filters.

Pei Xiao received the PhD degree from Chalmers University of Technology, Sweden in 2004. Prior to joining the University of Surrey in 2011, he worked as a research fellow at Queens University Belfast and had held positions at Nokia Networks in Finland. He is a Reader at University of Surrey and also the technical manager of 5G Innovation Centre (5GIC), leading and coordinating research activities, and overseeing major projects in all the work areas in 5GIC (http://www.surrey.ac.uk/5gic/research). Dr Xiaos research interests and expertise span a wide range of areas in communications theory and signal processing for wireless communications. He has published extensively in the field of wireless communications and in the cross-disciplinary areas of DSP and microwave propagation.

Jonathon A. Chambers (S'83-M'90-SM'98-F'11) received the Ph.D. and D.Sc. degrees in signal processing from the Imperial College of Science, Technology and Medicine (Imperial College London), London, U.K., in 1990 and 2014, respectively.

From 1991 to 1994, he was a Research Scientist with the Schlumberger Cambridge Research Centre, Cambridge, U.K. In 1994, he returned to Imperial College London as a Lecturer in signal processing and was promoted to Reader (Associate Professor) in 1998. From 2001 to 2004, he was the Director of the Centre for Digital Signal Processing and a Professor of signal processing with the Division of Engineering, Kings College London. From 2004 to 2007, he was a Cardiff Professorial Research Fellow with the School of Engineering, Cardiff University, Cardiff, U.K. Between 2007-2014, he led the Advanced Signal Processing Group, within the School of Electronic, Electrical and Systems Engineering and is now a Visiting Professor. In 2015, he joined the School of Electrical and Electronic Engineering, Newcastle University, where he is a Professor of signal and information processing and heads the ComS^{2}IP group. He is also a Guest Professor at Harbin Engineering University, China. He is a co-author of the books Recurrent Neural Networks for Prediction: Learning Algorithms, Architectures and Stability (New York, NY, USA: Wiley, 2001) and EEG Signal Processing (New York, NY, USA: Wiley, 2007). He has advised more than 60 researchers through to Ph.D. graduation and published more than 400 conference proceedings and journal articles, many of which are in IEEE journals. His research interests include adaptive and blind signal processing and their applications.

Dr. Chambers is a Fellow of the Royal Academy of Engineering, U.K., and the Institution of Electrical Engineers. He was the Technical Program Chair of the 15th International Conference on Digital Signal Processing and the 2009 IEEE Workshop on Statistical Signal Processing, both held in Cardiff, U.K., and a Technical Program Co-chair for the 36th IEEE International Conference on Acoustics, Speech, and Signal Processing, Prague, Czech Republic. He received the first QinetiQ Visiting Fellowship in 2007 for his outstanding contributions to adaptive signal processing and his contributions to QinetiQ, as a result of his successful industrial collaboration with the international defence systems company QinetiQ. He has served on the IEEE Signal Processing Theory and Methods Technical Committee for six years and the IEEE Signal Processing Society Awards Board for three years. He is currently a member of the IEEE Signal Processing Conference Board and the European Signal Processing Society Best Paper Awards Selection Panel. He has also served as an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING for three terms over the periods 1997-1999, 2004-2007, and since 2011 as a Senior Area Editor.